International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Different Audit Service to Ensure the Data Privacy and Integrity in Cloud Storage

Radhika H N[1], Simran R. Khiani[2]

[1] M.E Student, Department of CSE, G. H. Raisoni College of Engineering and Technology, University of Pune, India

[2] Assistant Professor, Department of IT, G. H. Raisoni College of Engineering and Technology, University of Pune, India

Abstract: ***Cloud computing is an emerging technology; it has gained an importance because of the advantages beyond this technology. The user will be using the software service provided by the cloud service provider without installing and maintaining it and user is paying purely based on his usage. Cloud storage technology frees the user from the load of local data storage and maintenance. The challenges of using cloud storage technology is the security issues involved while storing user data at the provider premises such as privacy and integrity . In this paper we are discussing about the different audit service which are used to ensure the privacy and integrity of the user data stored at cloud storage using a Third party auditor (TPA).***

Keywords: Cloud storage, Privacy, Integrity, Third Party auditor

1. Introduction

Cloud computing has created a kind of revolution in IT industry because of it's advantages such as location independent resource pooling , usage based pricing, On demand service, and rapid resource elasticity. There are mainly three different types of services provided by the cloud

- **Software as a service (SaaS)**
  The software service is provided by the cloud service provider to the user , with the help of this service the user can use the software hosted on the cloud server, without installing it at the user side .
- **Platform as a Service(PaaS)**
  The platform to the user to develop the application is provided by the cloud service provider. i.e., the middleware services and the operating system are provided to the user by the cloud service provider.
- **Infrastructure as a Service(IaaS)**
  The entire infrastructure is provided as a service to the user by the cloud service provider including storage, hardware, servers, networking components etc [16].

Let's consider the architecture of the cloud data storage service, The cloud data storage service consists of three different entities: Users, Cloud storage server, Third Party Auditor(TPA).

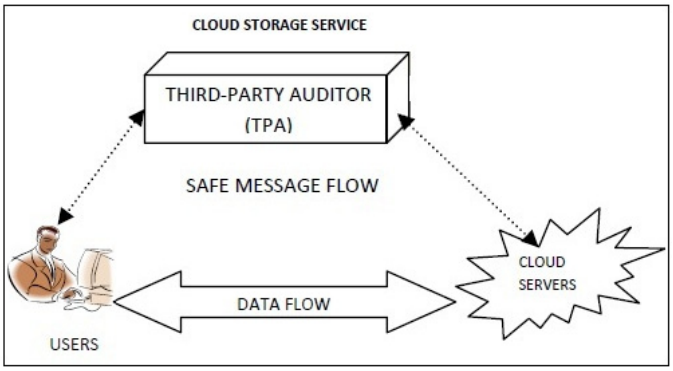

Figure 1: Architecture of cloud data storage service

- User: Users are the data owners who store their data in the storage provided by the cloud service provider.
- Cloud Storage Server: Cloud service provider manages the cloud storage servers. Cloud storage server provides space for user data storage.
- Third-Party Auditor: The TPA is an independent authority that has the capabilities and experience to monitor the integrity of the data outsourced on the cloud. It is trusted to access or expose the possibility of something bad happening in cloud storage services on behalf of client upon request [4].

Outsourcing data in the cloud provides the benefits like [18]. Makes the user free from the load of the storage management.

Data access is uniform, independent of geographical location.

Avoidance spending capital on hardware, software and personnel maintenance.

However, outsourcing of the data brings new security challenging issues [1]:

- Data privacy
- Data Integrity
- Entrusted cloud service provider

The first issue data privacy refers to the state that the user data stored in cloud is also known to someone else, he may be the other user of the cloud or cloud service provider itself or an attacker. The second issue data integrity refers to the state that exists when the computerized data is the same as that in the source document and not has been exposed to accidental or malicious alterations or destruction", there is no guarantee for the data stored in entrusted cloud server.

The third issue Entrusted cloud service provider, there are many reasons why the cloud service providers are not always trustworthy like, for saving the storage space and money, cloud service provider may discard the data that is not used for the long period of time or sometimes in order to maintain

the reputation cloud service provider may even hide the data losses or corruptions [18].

In order to ensure the integrity of outsourced data, data owner can provide the data auditing task to trusted third party auditor. The responsibilities of TPA are:

- Reducing the owner from the burden of managing the data
- Ensuring the owner that the data integrity of the data stored in the cloud is maintained.[13]

The TPA is an independent authority that has the capabilities and experience to monitor the integrity of the data outsourced on the cloud by meeting the following two fundamental requirements:

- TPA should be able to audit the cloud outsourced data efficiently without requiring the local copy of the data and thereby reducing the on-line burden of the cloud users.
- If there is any data corruption or loss the TPA informs the user. The TPA, should not affect privacy of the user data [10]

2. Different Audit Services

In [19] Wang .Q et.al (2009) the author mainly addresses the two major concerns with cloud data storage , one among them is data integrity verification at entrusted servers and the other is supporting dynamic data operation for cloud data storage applications. In Cloud Computing, the remotely stored electronic data is not accessed but also updated by the clients, e.g., through block insertion, deletion and modification. The remote data storage mainly focuses on static data files and the importance of dynamic data updates has received limited attention so far. Here the authors present an framework for public verifiability and data dynamic for cloud data storage and an efficient construction for seamless integration of these two components. Verification schemes are considered with public verifiability and the author assumes that the TPA is unbiased and the server is entrusted. The data privacy issues of cloud data storage is not addressed for application purposes, practically the client may often do block-level operations on the data files. The most general forms of these operations considered here are insertion, deletion, and modification. In the Proposed work there are mainly six different algorithms out of which three algorithms are run by the client and two algorithms are run by the server and one algorithm is run by either client or third party auditor (TPA).

- Client runs the key production algorithm it takes security parameter as an input and generates public and private key.
- Signature generation algorithm run by the client It takes private key as an input and a file which is an ordered collection of blocks and outputs the autograph set, it is an structured group of signatures on blocks. It also outputs metadata-the autograph of the source R of a Merkle hash tree. In our creation, the leaf nodes of the Merkle hash tree are hashes of file blocks.
- Data integrity proof algorithm is run by the server. a file , its signatures , and a challenge is taken as a file . It outputs a data integrity proof for the blocks specified.
- VerifyProof algorithm can be run by either the client or the third party auditor upon receipt of the proof. It takes public key, the challenge as an input, and the proof returned from the server, and outputs TRUE if the integrity of the file is verified as correct or FALSE otherwise.
- Server runs ExecUpdate algorithm. This takes a file, its signatures, and a data operation request as an input from client. It outputs an updated file, updated signatures and a proof for the operation.
- Client runs VerifyUpdate algorithm. Which takes public key, the signature, an operation request, and the proof Pupdate from server as an input and If the verification successes, it outputs a signature for the new root, otherwise false.

The third party auditor is used to check the integrity of outsourced data, to strongly bring in an efficient TPA, the auditing procedure should not bring new vulnerabilities towards user data privacy, and additional online burden to user should not be introduced. In [18] Wang.c et.al(2010) Proposed a secure cloud data storage system supporting privacy-preserving public auditing system and the TPA to do audits for several users concurrently and efficiently. The previous works not consider the privacy protection of users' data against external auditors. And they may potentially disclose client data information to the auditors. The skeleton for our privacy-preserving public auditing system consists of four algorithms: out of which two algorithms are run by the user, one algorithm is run by Server and the other algorithm is run by the TPA. The scheme is set up by running Key production algorithm run by the user. Signature generation algorithm is used by the user to produce certification metadata, which consist of linked data that will be used for auditing. Cloud server runs the Proof generation algorithm to generate a proof of information storage accuracy, and Proof verification algorithm is executed by the Third Party Auditor to audit the verification from the cloud server.

Running a public auditing system has two phases, Setup and Audit:

- Setup: The user initializes the public and private parameters of the system by executing Key generation algorithm, and pre-processes the data file by using Signature generation algorithm to produce the authentication metadata. The user then saves the data file and the authentication metadata at the cloud server, and erases its local copy. As component of pre-processing, the user may change content of the data file by escalating it or including extra metadata to be saved at server.
- Audit: The Third Party Auditor issues an audit note or challenge to the cloud server to create convinced that the cloud server has retained the data file correctly at the point of the audit. The cloud server will receive a reply note from a occupation of the stored data file and its verification metadata by executing Proof generation algorithm. The TPA then verifies the response via Proof verification algorithm.

In [15] Qian W et.al (2011) Proposed the scheme which is the extension of the [19] in the proposed scheme the authors presented the framework that is the integration of both Public auditability and data dynamic operation and extended [19] to support batch auditing where multiple request for auditing from different users can be performed by the TPA simultaneously, But the proposed scheme not considers the privacy issue of cloud security.

[5] Dalia Attas , Omar Batrafi (2011) the integrity is checked in 2 sides by TPA for outside attack and by cloud server for inside attack using digital signature with MD5 , But the cloud server is itself entrusted so the user data should not be exposed to the cloud server .

[12] K.Govinda, E.Sathiyamoorthy (2012) the Diffie-Hellman algorithm is used to generate secret key which is known to both user and auditor. The user performs XOR of data and secret key to generate cipher text, that cipher text is stored on cloud server. When the TPA want to check the integrity of outsourced data he takes the cipher text from the cloud which is XOR with secret key to get data. The user will do the hashing of data using SHA-1 hash function, the TPA also do the hashing of data using SHA-1 hash function , The hash value generated by the user and TPA is compared to check the integrity of the data , If both the hash value matches then the data is valid otherwise it is tampered, this scheme not considers the condition when many users are using auditing service provided by the third party auditor. And there is no mutual authentication between user and TPA.

[10] Jaspreet Kaur, Jasmeet singh (2013) the station-to-station protocol is used to generate secret key which is known to both user and auditor. The user performs XOR of data and secret key to generate cipher text, that cipher text is stored on cloud server. When the TPA wants to check the integrity of outsourced data he takes the cipher text from the cloud which is XOR with secret key to get data. The user will do the hashing of data using SHA-2 hash function, the TPA also do the hashing of data using SHA-2 hash function, The hash value generated by the user and TPA is compared to check the integrity of the data, If both the hash value matches then the data is valid otherwise it is tampered, There is a mutual authentication between user and TPA and the proposed scheme not considers the condition when many users are using auditing service provided by the third party auditor.

3. Conclusion

In this paper we discussed some of the research work from last five years involved to ensure data privacy and integrity in the cloud data storage using the different auditing service particularly using Third party auditor their pros and cons.

References

[1] Ateniese. G, Pietro. R.D, Mancini. L.V, Tsudik .G, "Scalable and efficient provable data possession", In: Proceedings of the 4th International Conference on Security and Privacy in Communication Networks , 2008.
[2] Ateniese . G, Burns. R.C, Curtmola. R, Herring. J, Kissner . L, Peterson. Z.N.J, Song. D.X, "Provable data possession at untrusted stores", In: Proceedings of the 2007 ACM Conference on Computer and Communications Security.
[3] Bowers, K.D, Juels, A , Oprea .A , 2009." Hail: a high-availability and integrity layer for cloud storage", In: ACM Conference on Computer and Communications Security, 2009.
[4] B.Dhiyanesh, A.Thiyagarajan, "A Novel Third Party Auditability and Dynamic Based Security in Cloud Compuitng", International Journal of Advanced Research in Technology(IJART), Vol. 1, Issue 1, 2011.
[5] Dalia Attas , Omar Batrafi , " Efficient integrity checking technique for securing client data in cloud computing " , International journal of Electrical and computer science , vol :11,no 5, 2011.
[6] Dodis . Y , Vadhan . S.P, Wichs .D, " Proofs of retrievability via hardness Amplification", 6th Theory of Cryptography Conference, 2009
[7] Erway .C . C , Küpc . ü . A , Papamanthou . C , Tamassia . R , "Dynamic provable data possession" , In: Proceedings of the 2009 ACM Conference on Computer and Communications Security, 2009.
[8] Fu . K , Kaashoek .M.F , Mazières .D , "Fast and secure distributed read-only file system" , ACM Trans. Comput. Syst. 20 (1), 1–24, 2002
[9] Hsiao . H . C , Lin . Y .H , Studer, A., Studer . C , Wang . K .H , Kikuchi . H , Perrig . A , Sun . H .M , Yang . B. Y , "A study of user-friendly hash comparison schemes" , In:ACSAC 2009.
[10] Jaspreet Kaur , Jasmeet singh , "Monitoring Data Integrity while using TPA in Cloud Environment ", International journal of Advanced Research in computer Engineering and Technology , vol 2 ,Issue 7 , July 2013.
[11] Juels .Jr , A , Kaliski . B.S , "Pors: proofs of retrievability for large files" . In: Proceedings of the 2007 ACM Conference on Computer and Communications Security , 2007.
[12] K.Govinda, E.Sathiyamoorthy, "Data Auditing in Cloud Environmen using Message Authentication Code", International Conference on Emerging Trends on Advanced Engineering Research(ICETT),2012.
[13] Miss .M.Sowparnika , Prof . Dheenadayalu , "Improving Data Integrity on Cloud Storage Service ", Internal journal of Engineering Science Invention , vol 2, Issue 2 , February 2013.
[14] Mell P . and Grance G. , "The NIST Definition of Cloud Computing (Draft) , " in Proceedings of the National Institute of Standards and Technology , Gaithersbuyg , pp.6 ,2011 .
[15] Qian Wang, Cong Wang, Kui Ren, Member, Wenjing Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing". IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.
[16] Shinha Rajak, Ashok Verma, "Secure Data Storage in the Cloud using Digital Signature Mechanism", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 1, Issue 4, June 2012.
[17] Shacham . H , Waters . B , "Compact proofs of retrievability" In: Advances in Cryptology – ASIACRY , 14th International Conference on the Theory and Application of Cryptology and Information Security , 2008.
[18] Wang.c , Wang . Q , Ren .K , Lou .w , " Privacy-preserving public auditing for data storage security in cloud computing " , In:INFOCOM , IEEE proceedings 2010 .
[19] Wang .Q, Wang . C , Li . J , Ren . K , Lou . W , "Enabling public verifiability and data dynamics for storage security in cloud computing. In: Proceedings of the 14th European Symposium on Research in Computer Security , 2009.
[20] Yan Zhu , HongXin Hu , Gail-Joon Ahn , Stephen s.yau , "Efficient audit Service outsourcing for data integrity in clouds ", The journal of system ans software , 2012.
[21] Yumerefendi . A.R , Chase . J.S , "Strong accountability for network storage", ACM Trans. Storage (TOS) 3 (3) , 2007.